Internet Messaging as a Family of Web Services

Kevin Lux (UPenn), Carl A. Gunter (UIUC), Raja N. Afandi (UIUC), Jianqing Zhang (UIUC)

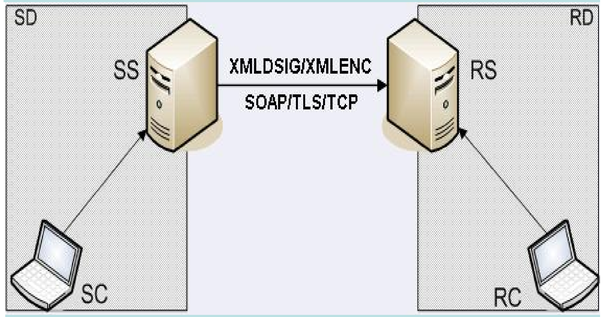
Illinois Security Lab

Motivation and Basic Idea

- Drawbacks of current Internet electronic mail:
  - Flexibility
  - Security
  - Integration
- Approach: Construct a Unified Messaging System based on Web Service Infrastructure
  - Standardized and Extensible
  - Widely adopted
  - Full-blown security specifications

Architecture

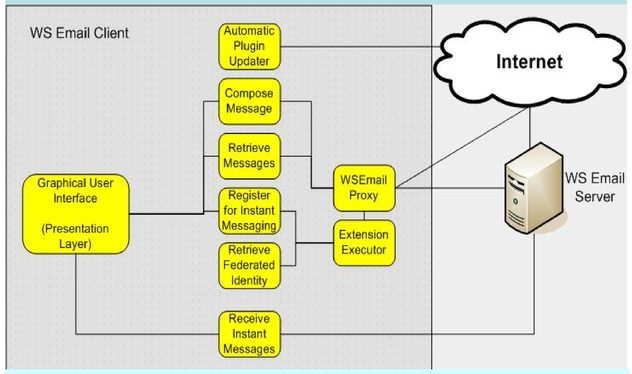
Distributed Components and Messages



- SD: Sender Domain
- SC: Sender Client
- SS: Sender Server
- RD: Receiver Domain
- RS: Receiver Server
- RC: Receiver Client

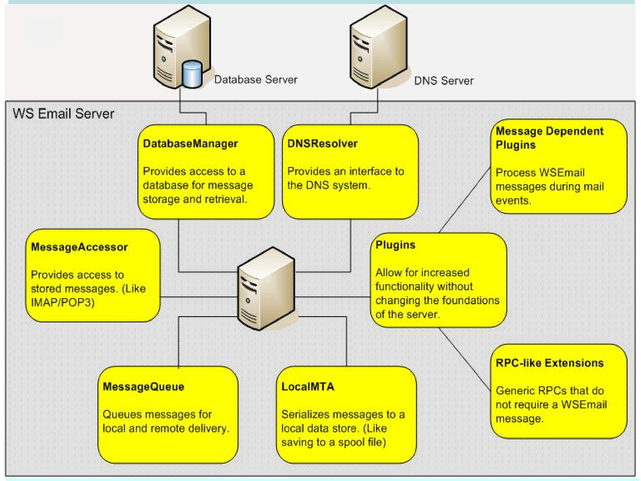
- SS/RS work as a web service.
- SC makes a web service call on its SS.
- SS makes a web service call on RS to deliver the mail from the SD into RD.
- RC periodically makes calls to RC to find new messages, retrieve message heads or download message bodies.
- Security is based on standard suites for web service security.
- Communications between the nodes can be protected by TLS.
- SC/RC are typically authenticated by password; SS /RS authenticate themselves by certificates.

Client



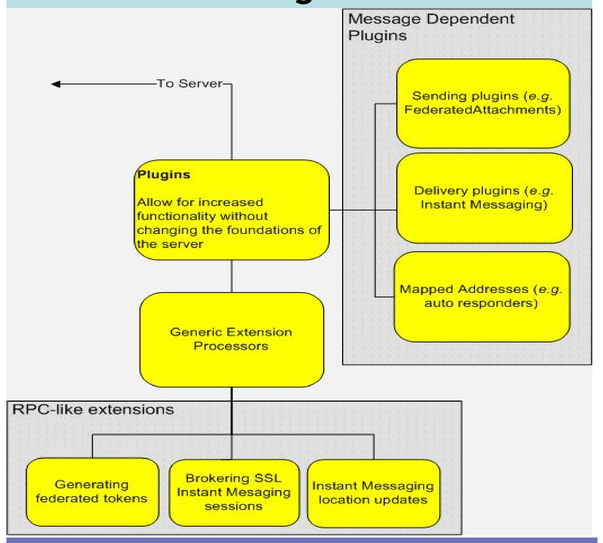
- Retrieve/read and compose/send messages.
- WSEmail Proxy takes local data and packages it up in to a SOAP request.
- Authenticate to the local server through a variety of security tokens: X509 certificate, username/password and federated identity token.
- Federated identities allow a client to send messages directly to the recipient's mail server.
- Plug-in inspects and downloads any attachments the message may contain. It has great benefits to distributed systems and for expanding client functionality on the fly.

Server



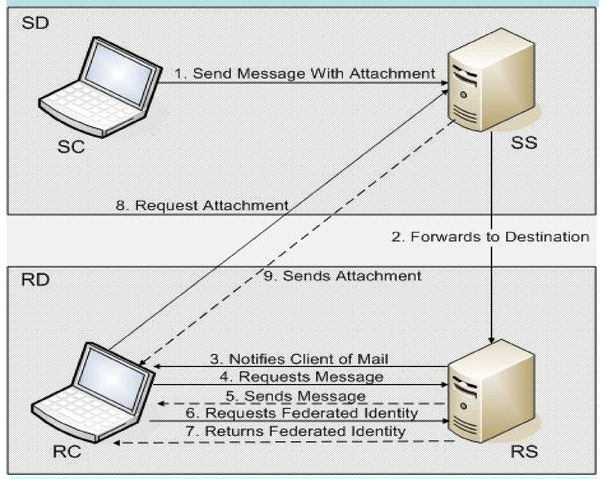
- Web server deals with receiving and distributing mails to both clients and other servers.
- Database server stores messages for the web server.
- DNS server publishes SRV records so that remote WSEmail servers can locate each other.

Plug-In



Application

On-Demand Attachments

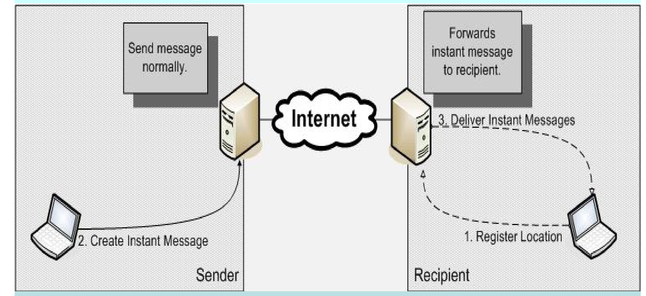


On-demand attachments allow a recipient to pull an attachment from the sender's server. This allows both sender and receiver more freedom. It also demonstrates the use of a federated identity system.

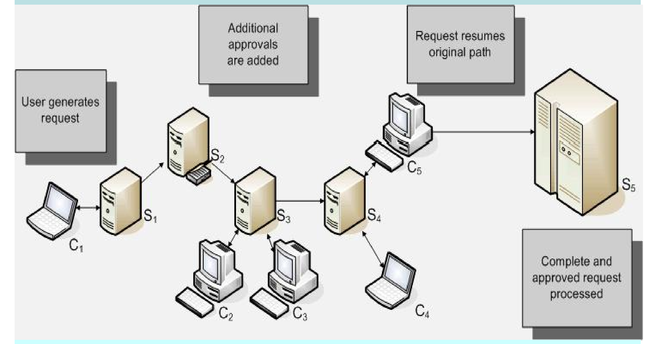
Instant Messaging

Unlike existing instant messaging systems, WSEmail treats instant message as a normal message, the only difference is how it is ultimately delivered.

Delivery of the message is intercepted by the instant messaging plug-in on the server and ultimately sent to the client through different means. Being a plug-in, a server admin can customize how instant messages are to be handled.



Routed Forms



Routed forms and distributed workflow systems could easily allow multiple enterprise to work together, even though their networks are not completely open and trusted by each other.

Achievements

- Security: supports integrity, authentication and access control for both end-to-end and hop-by-hop message transmissions using web service security features.
- Extensibility: integrates different messaging systems such as the usual email SMTP-style messages.
- Flexibility: collection of messaging services that can be added to the SOAP services.
- A unified messaging platform for new applications.

Future Work

- **Policy based puzzle anti-spam**
- Ingress and egress policy enforcement on mail servers
- Policy advertisement and negotiation
- Secure workflow
- Other research prototype project…

Motivation

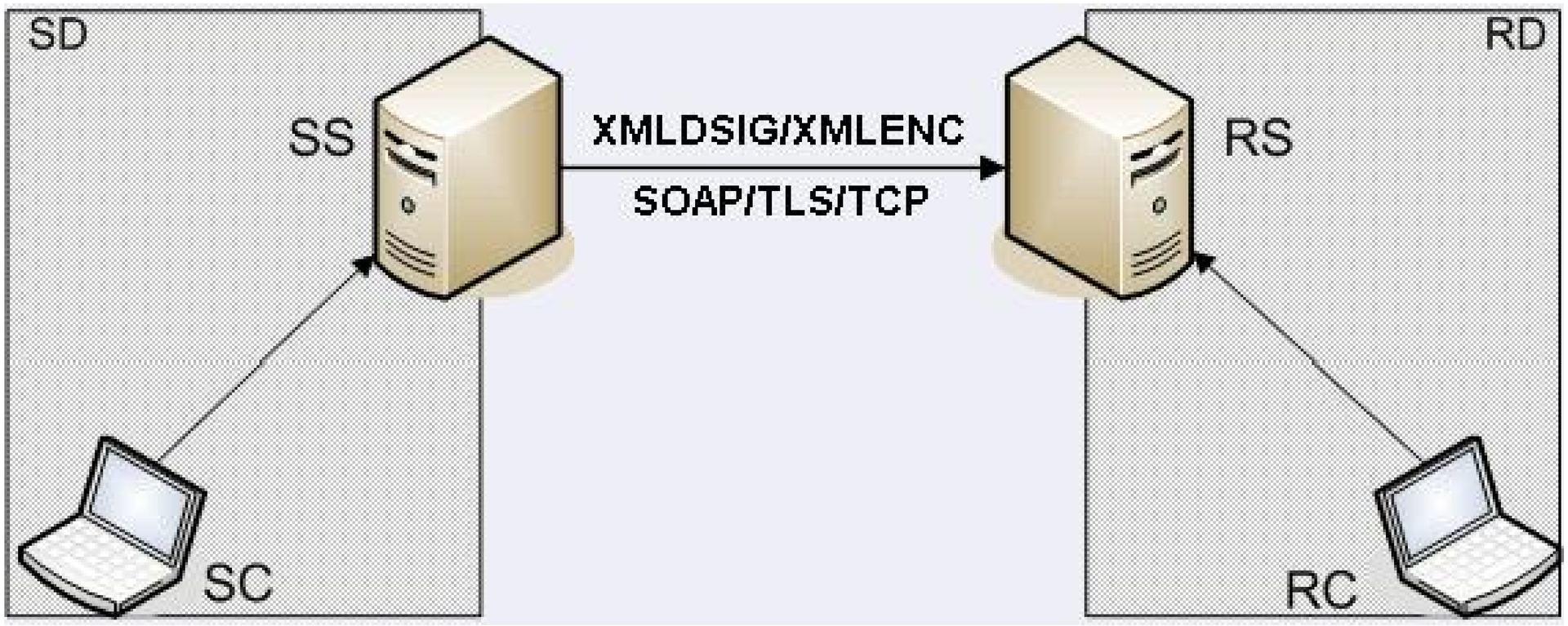
Illinois Security Lab

- Drawbacks of current Internet messaging systems:
  - Flexibility
  - Security
  - Integration
  - Scalability
- Approach: Construct a Unified Messaging System based on Web Service Infrastructure and XML Messaging
  - Standardized and Extensible
  - Scalable
  - Widely adopted
  - Full-blown security specifications

Architecture

Illinois Security Lab

Distributed Components and Messages



- SD: Sender Domain
- RD: Receiver Domain
- SC: Sender Client
- RS: Receiver Server
- SS: Sender Server
- RC: Receiver Client

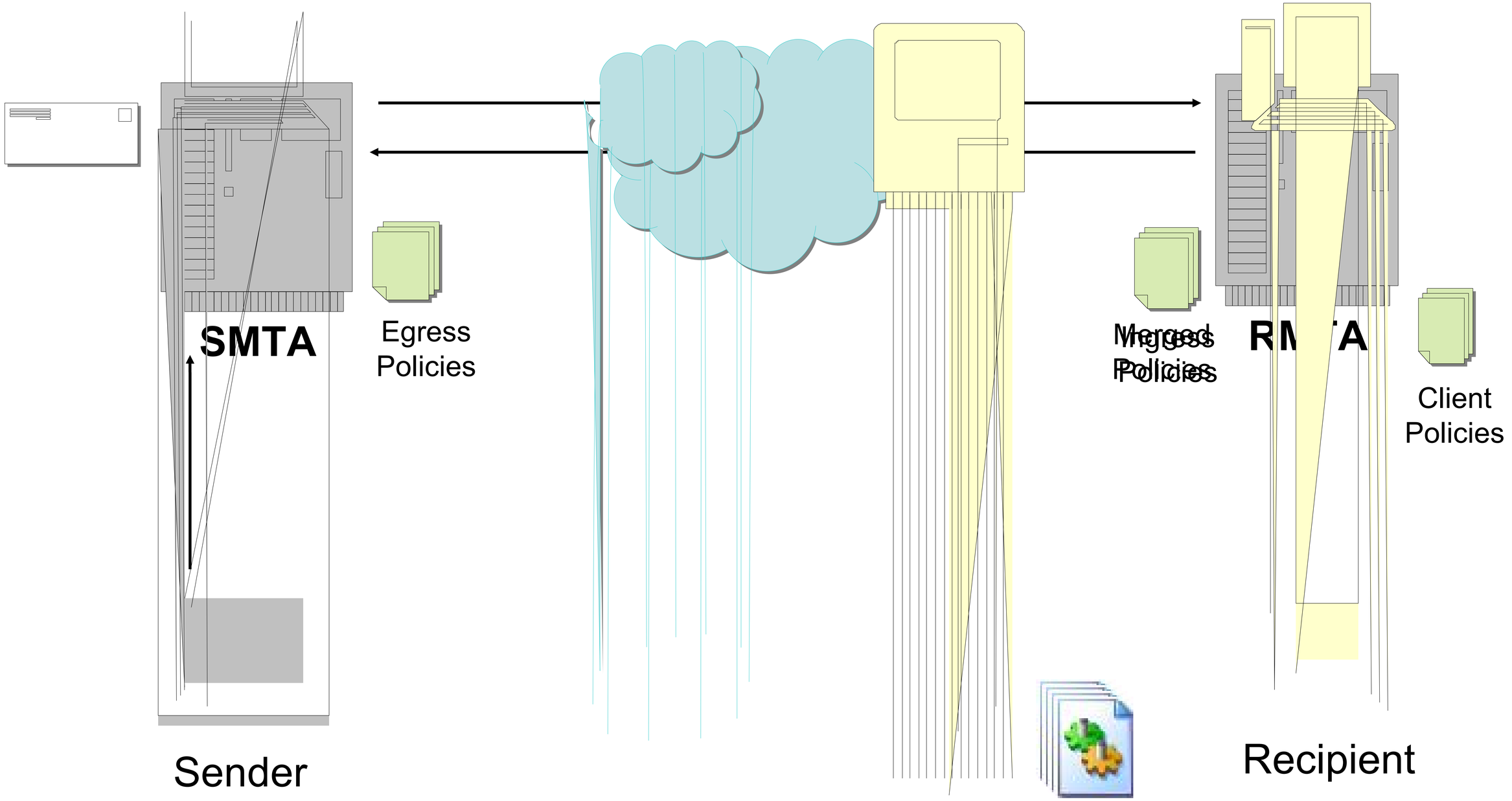
Architecture and Applications

Illinois Security Lab

- Plug-In
- Policy based email services
  - Ingress & Egress Policies
  - Policy Advertisement
  - Policy Negotiation
  - Policy Merging

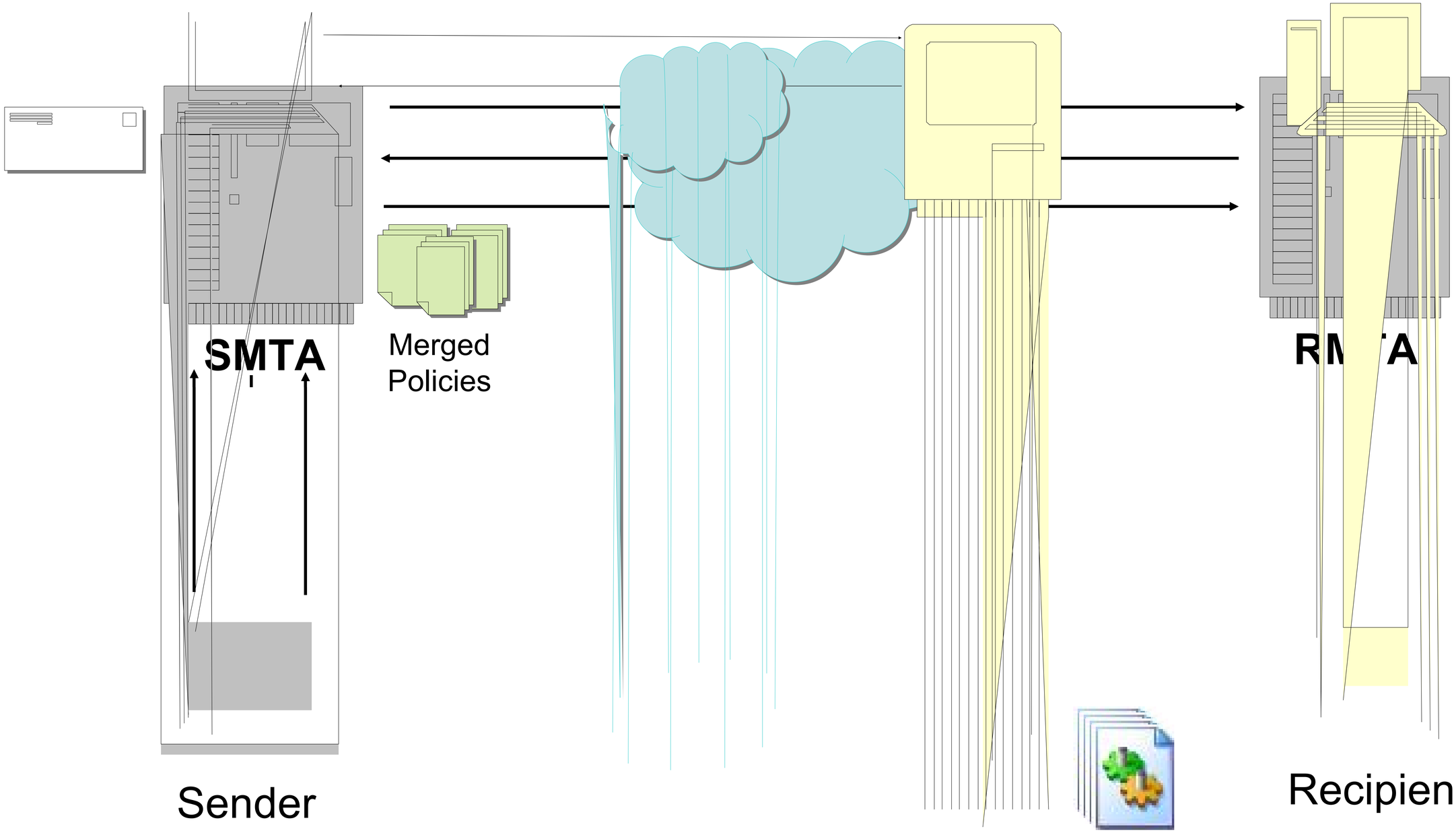
Policy Architecture

Illinois Security Lab



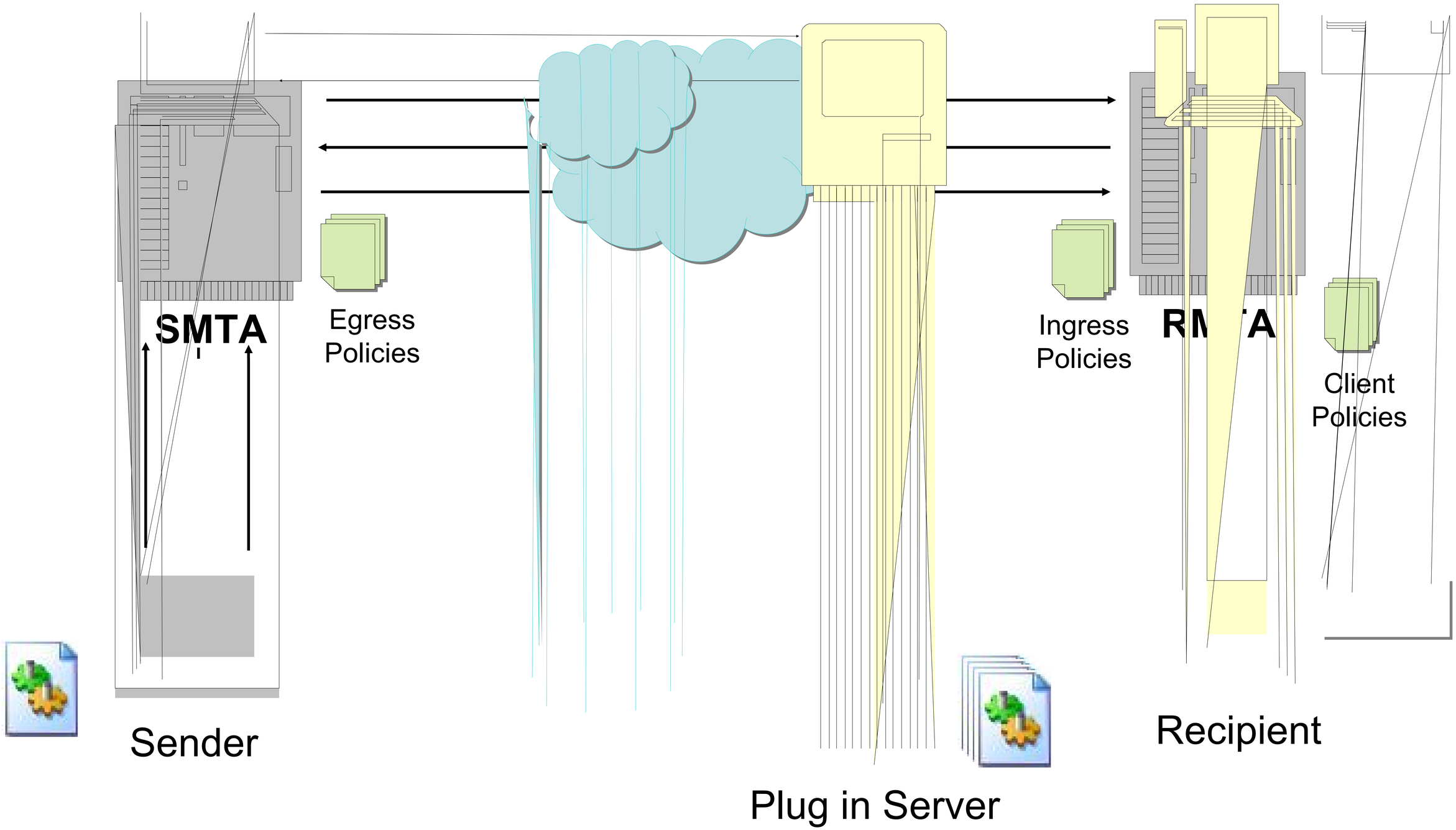
Policy Architecture

Illinois Security Lab



Policy Architecture

Illinois Security Lab



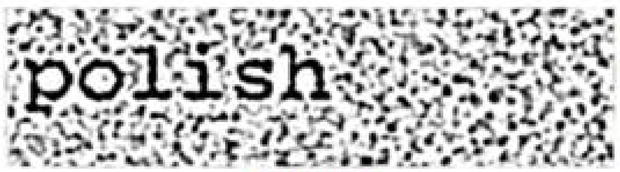
Puzzles

Illinois
Security Lab

- Puzzles
  - Increase cost of sending e-mail
  - Hash Cash
    - Usually non interactive
    - Computational puzzle
  - Reverse Turing Test (RTT)
    - Human interactive

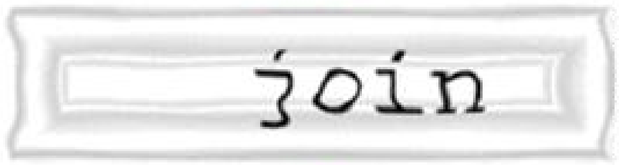
Puzzles

Illinois Security Lab

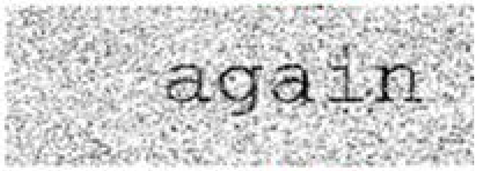


POLISH

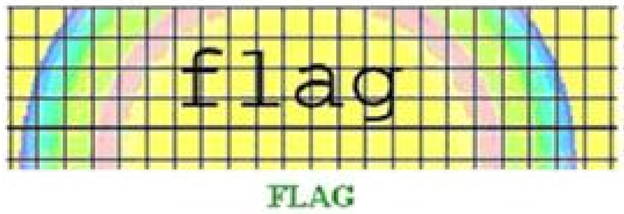
SPACE



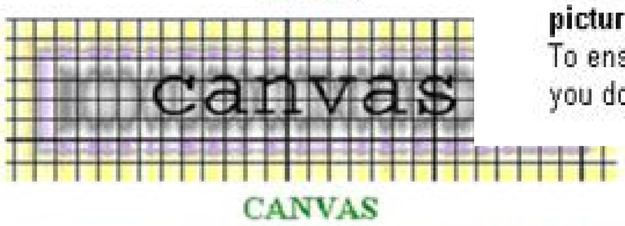
JOIN



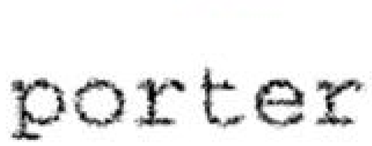
AGAIN



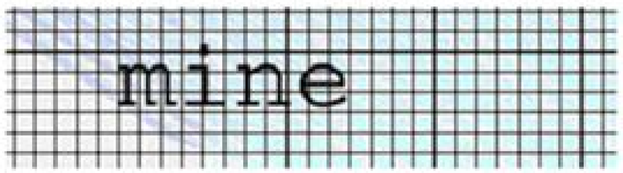
FLAG



CANVAS



PORTER



MINE

HORSE

JEWEL

WEIGHT

SOUND

YAHOO! Mail

Yahoo! - Help

Welcome to Yahoo! Mail

Login Failed.

Please use the correct password and type the word you see in the picture below.

Try the following hints.

- **You must enter the word you see in the picture.**
  To ensure the security of your account we require you do this after 5 failed attempts to login.

Existing Yahoo! users

Enter your ID and password to sign in

Yahoo! ID:

Password:

Issues & Future Work

Illinois Security Lab

- Policy specifications
- Complex negotiation and merging
- Privacy issues
- Integration with WS-* standards
- Secure workflow
- On-demand attachments